

REMARKS

Claims 1, 3-11 and 13-22 are pending. The Examiner's reconsideration of the rejection in view of the amendments and remarks is respectfully requested.

Claims 1-6, 9-16, 18 and 19-22 have been rejected under 35 U.S.C. 102(a) as being anticipated by Ober et al. (USPN 6,397,331). The Examiner stated essentially that Ober teaches all of the limitations of Claims 1-6, 9-16, 18 and 19-22.

Claims 1, 11 and 22 are the independent claims.

Claim 1 claims, *inter alia*, "a protected memory for storing authorized code, which contains an original digital signature, wherein said protected memory is cryptographically protected; and a processor in signal communication with said protected memory for preparing to execute code from the protected memory by verifying that a digital signature contained in said code is original in accordance with a public key, and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution." Claims 11 and 22 claim, *inter alia*, "applying an original digital signature to all authorized code; storing said signed authorized code in a protected memory, wherein said protected memory is cryptographically protected; preparing to execute code from the protected memory by verifying a digital signature used to sign said code in accordance with a public key, which corresponds to said original digital signature; and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code in said protected memory."

Ober teaches a method of expanding a secure kernel memory area to accommodate additional software code (see Abstract). Ober does not teach that a "protected memory is cryptographically protected" as claimed in Claim 1, nor "branching to a copy of said authorized

code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code is said protected memory” as claimed in Claims 11 and 22. Ober teaches that a secure kernel memory area may be expanded into an unprotected memory area (see col. 2, lines 28-34). Further, Ober teaches that the expansion may be in the form of a cryptographic algorithm or other kernel extension (see col. 2, lines 55-67). Such an expansion of secure kernel memory does not teach that the protected memory is cryptographically protected -- Ober teaches merely that the data in memory is signed. Signed data is not analogous to cryptographically protected memory as claimed in Claim 1, nor does it teach or suggest performing inline decryption of the copy of said authorized code is said protected memory as claimed in Claims 11 and 22. Indeed, nowhere to Ober teach cryptographically stored data – for example, the cryptographic algorithm stored in the newly acquired memory is not itself cryptographically protected. The data stored in the newly acquired memory of Ober is merely signed. Therefore, Ober fails to teach all the limitations of Claims 1, 11 and 22.

Claims 3-10 depend from Claim 1. Claims 13-21 depend from Claim 11. The dependent claims are believed to be allowable for at least the reasons given for the respective independent claims. Claims 2 and 12 have been cancelled. The Examiner’s reconsideration of the rejection is respectfully requested.

Claims 7, 8, 17 and 19 have been rejected under 35 USC 103(a) as being unpatentable over Ober in view of Ford et al. (USPN 5,481,613). The Examiner stated essentially that the combined teachings of Ober and Ford teach or suggest all the limitations of Claims 7, 8, 17 and 19.

Claims 7 and 8 depend from Claim 1. Claims 17 and 19 depend from Claim 11. The dependent claims are believed to be allowable for at least the reasons given for the respective independent claims. At least Claims 8 and 19 are believed to be allowable for additional reasons.

Claims 8 and 19 claim “wherein the privacy of said authorized code is protected at run time with symmetric key encryption.”

Ober teaches a method of expanding a secure kernel memory area to accommodate additional software code (see Abstract). Ober does not teach that “the privacy of said authorized code is protected at run time with symmetric key encryption” as claimed in Claims 8 and 19.

Ober teaches merely that the data in memory is signed. Signed data is not analogous to cryptographically protected memory as claimed in Claims 8 and 19. Nowhere to Ober teach cryptographically stored data. Therefore, Ober fails to teach all the limitations of Claims 8 and 19.


Ford teaches protected data communication between parties (see col. 2, lines 51-67). Ford does not teach or suggest that “the privacy of said authorized code is protected at run time with symmetric key encryption” as claimed in Claims 8 and 19. Ford’s method teaches communication of encrypted data. The mere communication of encrypted data is not analogous to protecting data at run time, essentially as claimed. For example, a decrypting party would have complete access to the data according to the teachings of Ford. Whereas, with run time encryption, a receiving party does not have unfettered access to the data but is still able to execute code. Therefore, Ford fails to teach or suggest all the limitations of Claims 8 and 19.

The combined teachings of Ober and Ford fail to teach or suggest that “the privacy of said authorized code is protected at run time with symmetric key encryption” as claimed in Claims 8 and 19. The Examiner’s reconsideration of the rejection is respectfully requested.

For the forgoing reasons, the application, including Claims 1, 3-11 and 13-22, is believed to be in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

Respectfully submitted,

Dated: February 15, 2007



Nathaniel T. Wallace
Reg. No. 48,909
Attorney for Applicants

F. CHAU & ASSOCIATES, LLC
130 Woodbury Road
Woodbury, New York 11797
TEL: (516) 692-8888
FAX: (516) 692-8889